



UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Australian Centre for
Health Engagement,
Evidence & Values

Response: Data Sharing and Transparency Bill & Accreditation Framework

The Australian Centre for Health Engagement Evidence and Values (ACHEEV) at the University of Wollongong recently conducted research on behalf of the Population Health Research Network (PHRN) to examine community attitudes towards governments sharing linked administrative health data sets with private companies for research and therapeutic development. Following this research, ACHEEV conducted two citizens' juries on the same topic.

In both the international literature and our survey, participants were ambivalent about whether or not to share their health data with private companies. Most people also wanted an opt-in approach for consent to release health data. By contrast, the citizens' juries supported sharing government health data with private industry for research and development, providing the intended purpose is clearly of public benefit, sharing occurs responsibly in a framework of accountability and the data are securely held. Many jurors shifted their perspective from complete opposition to recognition of the value of data sharing during the jury.

Our response is directed towards the inclusion of private industry as accredited data users, the development of appropriate levels of Australian ownership for an organisation to be eligible for accreditation, and transparency supported by public registers. Our response reflects our research on public attitudes towards sharing government administrative data with private industry, and public expectations of the additional safeguards required when sharing with private industry.

Accredited Data Users: Individuals and Organisations in the Private Domain

The level of public concern about commercial access to personal health data is sufficiently high to suggest that no unit level data (either identifiable or de-identified) should be released directly to a commercial entity. Our jury members supported the release of de-identified government administrative data (providing appropriate approval and review mechanisms were in place), but did not support the release of identifiable unit level data with private industry. We understand that commercial uses of public sector administrative data hold enormous promise in terms of development of new therapeutic interventions, assessing health services, monitoring safety and effectiveness of publicly-funded health technologies and comparative technology assessment. To support the concerns of the public, further developments of the accreditation framework may consider additional safeguards (and possible levels of restricted access) for accredited individual data users and/or accredited organisation data users employed in the private domain.

Although our jury did not focus on sharing government data with foreign entities, any suggestion of international access to administrative health data was met with great concern. In addition to concerns about access, the jurors were particularly concerned about data security.

Appropriate level of Australian Ownership for an Organisation to be Eligible for Accreditation as a Data Service Provider.

Further development of the appropriate level of Australian ownership for an organisation to be an accredited data user needs requires careful consideration of public attitudes towards foreign ownership and responsibility, the additional safeguards required, and costs involved in rectifying issues arising from foreign involvement.

We recommend accredited data service providers are based in Australia, Australian owned, and Australian run.

Transparency Supported by Public Registers

Transparency through an oversight body supported through public registries and data sharing agreements provides a strong foundation for governance and accountability. Findings from our juries indicate the public want to know who is accessing their data, how the data will be used, and what formal arrangements have been put in place to protect data. Our jurors also believed public knowledge of breaches and reporting of all results would enhance public trust.

In addition to hefty fines and penalties and exclusion of data sharing activities, our jurors believed misuse of data by private industry should be publicly disclosed. The jurors recognised that loss of privacy could be devastating to an individual and that penalties may not be sufficient to redress the wrong or to deter private companies from bad behaviour in the future. The jurors explicitly noted that large companies could easily afford the fines and penalties associated with a breach. They believed the damage to reputation through public registers of breaches would be seen as a greater harm to companies' reputations, and therefore would be more of a deterrent.

Although the juries supported the use of registers to make public details of which companies are accessing data, both juries were also cognisant of the commercial interests of private industry. They debated at length whether private companies should be required to share the results of their use of public data. Eventually, all jurors bar one agreed that all results should be shared with the oversight body. One jury also said the oversight body should share the results with the public if they believed it was in the public interest and/or of concern to the public.

Further legislation developments may need to consider whether the current registers extend to include the reporting of breaches and all results of government data sharing projects.

Community Engagement and Building Social Licence

Finally, we reflect again on how government administrative data should not be shared "where the Australian community does not support it". While the National Data Commissioner has provided ample opportunity for community feedback in a range of engagement activities, many of the individuals and organisations participating were not representative of our diverse country. Further efforts may be needed to consider, understand, inform and engage with a range of Australian voices, especially those from vulnerable and marginalised populations. This will lend support to the development of a social licence in the sharing of government data. Our research and the reported experience with the My Health Record release (Lupton, 2019) suggests:

- government will need to address the public's lack of understanding and lack of trust in the ways in which government agencies collect, share, protect and use their personal data.

- trust is built through ongoing transparent, interactive and informed engagement which takes into account the social context of the engagement, including capacity for and barriers to engagement

There are a range of ways in which we can engage on an ongoing way with the Australian community about sharing particular types of data. These include but are not limited to: population surveys; focus groups, particularly in vulnerable populations; public forums; publicly-focused websites for engagement and feedback; citizens' councils; and deliberative informed events such as citizens' juries. Government campaigns to communicate legislative changes will be part of the engagement. These strategies will provide information about public concerns and public values and will be crucial to the development of public understanding and a social licence for data sharing.

These strategies to engage the public must not be limited to the immediate future. Even once the Bill is passed, ongoing engagement with the public will be essential to maintain understanding and trust.

References:

Lupton, D. 2019. 'I'd like to think you could trust the government, but I don't really think we can': Australian women's attitudes to and experiences of My Health Record. *Digital Health*, 5:1-12.